IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Banerjee, et. al.	§ Group Art Unit: 2141
	§ Confirmation No.: 1787
	§ Examiner: Bayard, Djenane M
Serial No.: 09/870,610	§
	§ Attorney Docket No.
Filed: May 31, 2001	§ AUS920010361US1
	§
Title: System and Method for Extending Server Security Through Monitored Load Management	§ IBM Corporation § Intellectual Property Law § Dept. § 11400 Burnet Road § Austin, Texas 78758

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Mailing or Transmission

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 or electronically transmitted to the U.S. Patent and Trademark Office on the date shown below.

/Leslie A. Van Leeuwen, Reg. No. 42,196/ August 25, 2006
Leslie A. Van Leeuwen, Reg. No. 42,196 Date

AMENDED APPELLANTS' BRIEF (37 CFR § 41.37)

Sir:

A. INTRODUCTORY COMMENTS

This amended appeal brief is filed in response to the Notification of Non-Compliant Appeal Brief mailed on August 11, 2006. Appellants have revised the Summary of Claimed Subject Matter to more clearly provide a concise explanation of independent claims 8 and 14, as required by the Notification. In addition, Appellants have included a separate argument for each ground of rejection.

This brief is filed in support of the previously filed Notice of Appeal, filed in this case on June 5, 2006, which appealed from the decision of the Examiner dated March 3, 2006, finally rejecting claims 1, 5, 8, 11, 14, 18, and 21-30. Appellants respectfully request that the fee for the originally filed Appeal Brief, filed on July 24, 2006, be applied to the filing of this Amended Appeal Brief. Therefore, no fee is believed due for the filing of the present Appeal Brief.

No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and the undersigned hereby authorizes the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

B. REAL PARTY IN INTEREST

The real party in interest in this appeal is International Business Machines Corporation, which is the assignee of the entire right, title, and interest in the above-identified patent application.

C. RELATED APPEALS AND INTERFERENCES

With respect to other prior or pending appeals, interferences, or judicial proceedings that are related to, will directly affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such prior or pending appeals, interferences, or judicial proceeding known to Appellants, Appellants' legal representative, or assignee.

D. STATUS OF CLAIMS

1. Total number of claims in application

There are 16 claims pending. Four claims are independent claims (1, 8, 14, and 27), and the remaining claims are dependent claims.

2. Status of all claims in application

- Claims canceled: 2-4, 6-7, 9-10, 12-13, 15-17, and 19-20
- Claims withdrawn from consideration but not canceled: none
- Claims pending: 1, 5, 8, 11, 14, 18, and 21-30
- Claims allowed: None
- Claims rejected: 1, 5, 8, 11, 14, 18, and 21-30

3. Claims on appeal

Claims 1, 5, 8, 11, 14, 18, and 21-30 are on appeal.

E. STATUS OF AMENDMENTS

All amendments have been entered in this case. No amendments have been made to the claims after the Final Office Action.

F. SUMMARY OF CLAIMED SUBJECT MATTER

Appellants provide a concise summary of the claimed subject matter as follows. Claims 1, 8, 14, and 27 are independent claims. Note that claims 1, 5, 21, 22, 27, and 28 are method claims, claims 8, 11, 23-24, and 29 are information handling system claims, and claims 14, 18, 25-26, and 30 are computer program product claims. Independent claims 8 and 14 include logic elements and means plus function limitations that correspond to the method steps set forth in independent claim 1. An information handling system capable of implementing Appellants' invention, as claimed in independent claim 8, is shown in Figure 7, and described in Appellants' specification on page 17, line 11 - page 18, line 24. Support for independent computer program product claim 14 is described in Appellants' specification on pages 18-19. In addition, support for each of the method steps, logic elements, and means plus function limitations of the independent claims are discussed below. The specific citations to Appellants' Figures and Specification are meant to be exemplary in nature, and do not limit the scope of the claims. In particular, the citations below do not limit the scope of equivalents as provided under 35 U.S.C. § 112, sixth paragraph.

As claimed in independent claim 1, Appellants claim a method for providing a test script, the test script including one or more attack simulations (See Figure 3, reference numeral 320; page 11, line 22 through page 13, line 8); processing the attack simulations included in the test script (See Figure 3, reference numerals 320 and 330; page 11, line 22 through page 13, line 8); determining whether to change one or more configuration settings based upon the processing (See Figure 3, reference numerals 340, 350, and 360; page 11, line 22 through page 13, line 8); changing one or more of the configuration settings based upon the determination (See Figure 3,

reference numerals 355 and 365; page 11, line 22 through page 13, line 8); receiving a packet from a client computer (See Figure 1, reference numeral 140; page 8, line 8 through page 9, line 14; Figure 2, reference numeral 250; page 9, line 15 through page 11, line 21; Figure 4, reference numeral 420; and page 13, line 9 through page 15, line 4); identifying the client computer by a source IP address (See Figure 4, reference numeral 430; page 13, line 9 through page 15, line 4); calculating a number of packets received using the source IP address during a time interval (See Figure 4, reference numeral 420; page 13, line 9 through page 15, line 4), wherein the calculating includes: retrieving a number of packets received that correspond to the source IP address (See Figure 4, reference numeral 470; page 13, line 9 through page 15, line 4); and incrementing the number of packets received (See Figure 4, reference numeral 470; page 13, line 9 through page 15, line 4); comparing the incremented number of packets received with one or more of the configuration settings (See Figure 4, reference numeral 480; page 13, line 9 through page 15, line 4); determining an action from a plurality of actions based on the comparing (See Figure 6, reference numeral 610 and 620; page 16, line 13 through page 17, line 10); and executing the action (See Figure 6, reference numerals 615, 624, 628, and 630; page 16, line 13 through page 17, line 10).

As claimed in independent claim 8, Appellants claim an information handling system (See Figure 7, reference numeral 701; page 17, line 11 through page 18, line 24), one or more processors (See Figure 7, reference numeral 700; page 17, line 11 through page 18, line 24); a memory accessible by the processors (See Figure 7, reference numerals 710 and 720; page 17, line 11 through page 18, line 24); one or more nonvolatile storage devices accessible by the processors (See Figure 7, reference numeral 772; page 17, line 11 through page 18, line 24); a network interface for receiving packets from a computer network (See Figure 7, reference numerals 745 and 750; page 17, line 11 through page 18, line 24); and a packet handling tool to manage packets received from the network interface (See Figure 2, reference numeral 200; page 9, line 15 through page 11, line 21), the packet handling tool including: means for providing a test script, the test script including one or more attack simulations (See Figure 3, reference numeral 320; page 11, line 22 through page 13, line 8; Figure 7, reference numerals 700 and 772, page 17, line 11 through page 18, line 24); means for processing the attack simulations included in the test script (See Figure 3, reference numerals 320 and 330; page 11, line 22 through page

13, line 8; Figure 7, reference numerals 700 and 772, page 17, line 11 through page 18, line 24); means for determining whether to change one or more configuration settings based upon the processing (See Figure 3, reference numerals 340, 350, and 360; page 11, line 22 through page 13, line 8; Figure 7, reference numerals 700 and 772, page 17, line 11 through page 18, line 24); means for changing one or more of the configuration settings based upon the determination (See Figure 3, reference numerals 355 and 365; page 11, line 22 through page 13, line 8; Figure 7, reference numerals 700 and 772, page 17, line 11 through page 18, line 24); means for receiving a packet from a client computer (See Figure 1, reference numeral 140; page 8, line 8 through page 9, line 14; Figure 2, reference numeral 250; page 9, line 15 through page 11, line 21; Figure 4, reference numeral 420; and page 13, line 9 through page 15, line 4; Figure 7, reference numerals 700 and 772, page 17, line 11 through page 18, line 24); means for identifying the client computer by a source IP address (See Figure 4, reference numeral 430; page 13, line 9 through page 15, line 4; Figure 7, reference numerals 700 and 772, page 17, line 11 through page 18, line 24); means for calculating a number of packets received using the source IP address during a time interval (See Figure 4, reference numeral 420; page 13, line 9 through page 15, line 4; Figure 7, reference numerals 700 and 772, page 17, line 11 through page 18, line 24), wherein the calculating includes: means for retrieving a number of packets received that correspond to the source IP address (See Figure 4, reference numeral 470; page 13, line 9 through page 15, line 4; Figure 7, reference numerals 700 and 772, page 17, line 11 through page 18, line 24); and means for incrementing the number of packets received (See Figure 4, reference numeral 470; page 13, line 9 through page 15, line 4; Figure 7, reference numerals 700 and 772, page 17, line 11 through page 18, line 24); means for comparing the incremented number of packets received with one or more of the configuration settings (See Figure 4, reference numeral 480; page 13, line 9 through page 15, line 4; Figure 7, reference numerals 700 and 772, page 17, line 11 through page 18, line 24); means for determining an action from a plurality of actions based on the comparing (See Figure 6, reference numeral 610 and 620; page 16, line 13 through page 17, line 10; Figure 7, reference numerals 700 and 772, page 17, line 11 through page 18, line 24); and means for executing the action (See Figure 6, reference numerals 615, 624, 628, and 630; page 16, line 13 through page 17, line 10; Figure 7, reference numerals 700 and 772, page 17, line 11 through page 18, line 24).

As claimed in independent claim 14, Appellants claim a computer program product (See pages 18-19) stored on a computer operable media (See Figure 7, reference numerals 710, 720, and 772, page 17, line 11 - page 18, line 24), the computer operable media containing instructions for execution by a computer (See pages 18-19), which, when executed by the computer, cause the computer to implement a method for preventing malicious attacks, the method comprising: providing a test script, the test script including one or more attack simulations (See Figure 3, reference numeral 320; page 11, line 22 through page 13, line 8); processing the attack simulations included in the test script (See Figure 3, reference numerals 320 and 330; page 11, line 22 through page 13, line 8); determining whether to change one or more configuration settings based upon the processing (See Figure 3, reference numerals 340, 350, and 360; page 11, line 22 through page 13, line 8); changing one or more of the configuration settings based upon the determination (See Figure 3, reference numerals 355 and 365; page 11, line 22 through page 13, line 8); receiving a packet from a client computer (See Figure 1, reference numeral 140; page 8, line 8 through page 9, line 14; Figure 2, reference numeral 250; page 9, line 15 through page 11, line 21; Figure 4, reference numeral 420; and page 13, line 9 through page 15, line 4); identifying the client computer by a source IP address (See Figure 4, reference numeral 430; page 13, line 9 through page 15, line 4); calculating a number of packets received using the source IP address during a time interval (See Figure 4, reference numeral 420; page 13, line 9 through page 15, line 4), wherein the calculating includes: retrieving a number of packets received that correspond to the source IP address (See Figure 4, reference numeral 470; page 13, line 9 through page 15, line 4); and incrementing the number of packets received (See Figure 4, reference numeral 470; page 13, line 9 through page 15, line 4); comparing the incremented number of packets received with one or more of the configuration settings (See Figure 4, reference numeral 480; page 13, line 9 through page 15, line 4); determining an action from a plurality of actions based on the comparing (See Figure 6, reference numeral 610 and 620; page 16, line 13 through page 17, line 10); and executing the action (See Figure 6, reference numerals 615, 624, 628, and 630; page 16, line 13 through page 17, line 10).

As claimed in independent claim 27, Appellants claim a method for preventing malicious network attacks on a server computer from a client computer that accesses the server computer

via a computer network comprising the steps of executing a test script that includes one or more attack simulations from the client computer (Se Figure 3, reference numeral 330; page 11, line 22 through page 13), the execution of the test script including: receiving, at the server computer, one or more packets from the client computer and one or more open socket requests form the client computer (See Figure 4, reference numeral 420; page 13, line 9 through page 15, line 4); deciding a packet threshold for the client computer (See Figure 3, reference numeral 340; page 11, line 22 through page 13, line 8), the deciding including: determining a number of packets received from the client computer during a time interval (See Figure 4, reference numeral 470; page 13, line 9 through page 15, line 4); incrementing the number of packets received from the client computer (See Figure 4, reference numeral 470; page 13, line 9 through page 15, line 4); and comparing the number of packets received with a packet limit stored at the server computer (See Figure 4, reference numeral 480; page 13, line 9 through page 15, line 4); computing an open socket threshold for the client computer (See Figure 5, reference numeral 550; page 15, line 5 through page 16, line 12), the computing including: determining a number of opened sockets for the client computer (See Figure 5, reference numeral 550; page 15, line 5 through page 16, line 12); incrementing the number of opened sockets for the client computer (See Figure 5, reference numeral 550; page 15, line 5 through page 16, line 12); comparing the number of sockets opened from the client computer to a socket limit stored at the server computer (See Figure 5, reference numeral 560; page 15, line 5 through page 16, line 12); and evaluating the packet limit and the socket limit used during the attack simulations (See Figure 3, reference numeral 330; page 11, line 22 through page 13, line 8), the evaluating including: analyzing the performance of the server computer during the simulation (Figure 3, reference numeral 330; page 11, line 22 through page 13, line 8); and adjusting a server configuration setting based on the analysis, wherein the adjusted server configuration setting is selected from group consisting of the stored packet limit and the stored socket limit (See Figure 3, reference numerals 335 and 365; page 11, line 22 through page 13, line 8).

Appellants argue the claims in several groups, and, as required by 37 C.F.R. §41.37(c)(1)(v), Appellants provide support from the specification for the means plus function elements of each dependent claim argued separately below.

Dependent claim 23 is argued separately below (as part of a group including claims 21, 23, and 25) and includes wherein the configuration settings include a first limit and a second limit (See Figure 3, reference numeral 31; page 11, line 22 through page 13, line 8); means for determining that the incremented number of packets exceeds the first limit (See Figure 6, reference numerals 610 and 620; page 16, line 13 through page 17, line 10; Figure 7, reference numerals 700 and 772, page 17, line 11 through page 18, line 24); means for processing the packet and sending a notification in response to determining that the incremented number of packets exceeds the first limit (See Figure 6, reference numerals 624 and 628; page 16, line 13 through page 17, line 10; Figure 7, reference numerals 700 and 772; page 17, line 11 through page 18, line 24); means for receiving a subsequent packet from the client computer (See Figure 4, reference numeral 420; page 13, line 9 through page 15, line 4; Figure 7, reference numerals 700 and 772; page 17, line 11 through page 18, line 24); means for incrementing again the number of packets in response to receiving the subsequent packet (See Figure 4, reference numeral 470; page 13, line 9 through page 15, line 4; Figure 7, reference numerals 700 and 772; page 17, line 11 through page 18, line 24); means for determining that the incremented again number of packets exceeds the second limit (See Figure 6, reference numeral 610; page 16, line 13 through page 17, line 10; Figure 7, reference numerals 700 and 772; page 17, line 11 through page 18, line 24); and means for rejecting the subsequent packet in response to determining that the incremented again number of packets exceeds the second limit (See Figure 6, reference numeral 624; page 16, line 13 through page 17, line 10; Figure 7, reference numerals 700 and 772; page 17, line 11 through page 18, line 24).

Dependent claim 24 is argued separately below (as part of a group including claims 22, 24, and 26) and includes wherein the configuration settings include a historical usage corresponding to the client computer (See page 6, lines 5 through 13; Figure 7, reference numerals 700 and 772, page 17, line 11 through page 18, line 24); means for determining that the incremented number of packets is higher than the historical usage (See Figure 4, reference numeral 480; page 13, line 9 through page 15, line 4; Figure 7, reference numerals 700 and 772, page 17, line 11 through page 18, line 24); and means for sending a notification in response to determining that the incremented number of packets is higher than the historical usage (See

Figure 6, reference numeral 624; page 16, line 13 through page 17, line 10; Figure 7, reference numerals 700 and 772, page 17, line 11 through page 18, line 24).

G. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1, 5, 8, 11, 14, 18, and 28-30 on appeal stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Lewis et al. (U.S. Patent Pub. 2003/0110396, hereinafter "Lewis") in view of Lockhart et al. (U.S. Patent No. 6,189,035, hereinafter "Lockhart"). Claims 21, 23, and 25 on appeal stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Lewis in view of Lockhart and further in view of Carlson (U.S. Patent No. 6,381,649, hereinafter "Carlson"). Claims 22, 24, and 26 on appeal stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Lewis in view of Lockhart and further in view of Porras et al. (U.S. Patent No. 6,321,338, hereinafter "Porras"). Claim 27 on appeal stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Ptacek et al. (U.S. Patent No. 6,636,972, hereinafter "Ptacek") in view of Lockhart and further in view of Barrett et al. (U.S. Patent Pub. 2002/0059454, hereinafter "Barret").

H. ARGUMENT

1. Claims 1, 5, 8, 11, 14, 18, and 28-30 Are Patentable over Lewis in view of Lockhart.

Independent claims 1, 8, and 14 claim a method, system, and program product for preventing malicious network attacks. Using claim 1 as an exemplary claim, each of these independent claims includes the limitations of:

1) providing a test script, the test script including one or more attack simulations;

2) processing the attack simulations included in the test script;

3) determining whether to change one or more **configuration settings** based upon the processing;

4) changing one or more of **the configuration settings** based upon the determination;

5) receiving a packet from a client computer;

6) identifying the client computer by a source IP address;

7) calculating a number of packets received using the source IP address during a time interval, wherein the calculating includes:

8) retrieving a number of packets received that correspond to the source IP address; and

9) incrementing the number of packets received;

10) comparing the incremented number of packets received with one or more of **the configuration settings**;

11) determining an action from a plurality of actions based on the comparing; and

12) executing the action.

Appellants use an attack simulation test script to adjust a server's configuration settings for security purposes (first through fourth elements), such as adjusting a number of packets that the server allows from a source IP address in a given amount of time. Once configured, Appellants track the number of packets that the server receives from a particular source IP address (fifth through ninth elements) and compare the source IP address' total number of packets with the **same** configuration settings that were adjusted during the test script simulation (tenth element). Finally, Appellants determine whether to perform an action (block the packet, notify an administrator, etc.) based upon the comparing, and execute the action (eleventh through twelfth elements).

Appellants assert that the Examiner fails to establish a prima facie case of obviousness under § 103 as set forth in § 103 and the MPEP. MPEP 2142 states that "To establish a prima facie case of obviousness… **there must be a reasonable expectation of success**." Appellants assert that when combining Lewis with Lockhart, the combination does not result in a reasonable expectation of success, which is discussed in detail below.

In addition, Appellants assert that the Examiner fails to show that the prior art references teach or suggest all of Appellants' claim limitations. In particular, Appellants assert that the

Examiner fails to view Appellants' invention as a "whole." MPEP 2141 states that "When applying 35 U.S.C. 103, the following tenets of patent law must be adhered to: (A) The claimed invention must be considered **as a whole**…" In addition, MPEP 2143.03 states:

> "To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art…**All words** in a claim must be considered in judging the patentability of that claim against the prior art" (emphasis added)

Appellants assert that the Examiner fails to consider all words in Appellants' claims as a whole during the Examiner's patentability judgment. Appellants clearly claim "**configuration settings**" in Appellants' third element, and "**the configuration settings**" in Appellants' fourth and tenth elements. Hence, Appellants are claiming the **same** configuration settings in each of these elements. Appellants assert, however, that the Examiner does not view Appellants' "configuration settings" on a consistent basis for each element and, therefore, the Examiner does not view Appellants' claim 1 as a whole (discussed below).

The Examiner uses Lewis to reject claim 1's first through fourth elements. During these rejections, the Examiner uses Lewis' "triggers," which Lewis associates with "precursors," to reject Appellants' "configuration settings" limitation. Particularly, Lewis states:

> "A monitor continuously checks for the presence of the identified **precursors**. When the monitor detects the presence of a precursor, appropriate action is taken. On or more triggers responsive to the detection of the identified precursors may be incorporated into the network or network devices. In this case, when the monitor detects the presence of a precursor, one or more of the triggers signal the action-taking means to take appropriate protective action." (page 2, para. 18, emphasis added)

Lewis defines attack precursors as events that occur prior to an attack that are identifiable. Lewis states:

> "As previously discussed, almost all security violations encountered in practice evolve in multiple stages, and some of the preliminary stages may not be destructive per se but rather merely preparatory steps in the attach scenario. If indicators of these preparatory steps, or "attack precursors," can be detected and immediate action is then taken, the resulting attack may be prevented." (page 3, para. 37, emphasis added)

> "Detection of the presence of a precursor triggers protective action…This provides an advantage because the time lapse between detection of a precursor event and the onset of an attack may be on the order of **minutes to seconds**." (page 4, para. 49, emphasis added)
>
> "Once the general nature of the type of attacks of interest are understood, experiments are set up in which (i) attacks are simulated, (ii) data is collected from all systems involved, and (iii) the data is analyzed with statistical algorithms in order to determine probable precursors of target shutdowns." (page 6, para. 65)
>
> "…the variables icmpInMsgs, icmpInEchos, icmpInEchoReps, and icmpOutEchos are key variables for detecting Ping Flood Attacks since they are related to the inflows of pings (ICMP Echo Request messages) in the target machine." (page 6, para. 75)

As can be seen, Lewis' precursors are identified events prior to an attack that indicate the onset of an attack. Lewis' precursors, however, are not based upon source IP addresses because, for example, Lewis states, "*Recall that it is not known which ones are the attacking machines…*" (page 7, para. 87). Since the Examiner uses these precursors to reject Appellants' configuration settings limitation, the Examiner must continue to use Lewis' precursors when viewing each of Appellants' subsequent configuration settings limitations in order to view Appellants' claim 1 as a whole (discussed below).

The Examiner uses Lockhart to reject claim 1's fifth through twelfth elements. Claim 1's tenth element claims "comparing the incremented number of packets received with one or more of **the configuration settings**." Appellants note that these configuration settings are the **same** configuration settings that are changed in claim 1's fourth element. In reviewing the Examiner's rejection, the Examiner uses Lockhart that states "*a determination is made as to whether the recent packet count for this particular IP source exceeds a predetermined threshold*" (See the Final Office Action on page 4, lines 14-15, emphasis added). The Examiner's reasoning in using this statement, however, is flawed in two areas. First, Lockhart uses a **predetermined** threshold in which Lockhart never teaches or suggests changing the predetermined threshold based upon attack simulations as claimed by Appellants. Second, by combining Lewis and Lockhart and viewing claim 1 as a whole, the combination results in Lockhart comparing the recent packet count to Lewis' precursors because Lewis' precursors must be used when viewing Appellants' "configuration settings" limitation throughout Appellants' claim 1 (discussed above). As

discussed above, Lewis' precursors are not based upon a number of packets received from a particular source IP address and, therefore, the combination of Lewis and Lockhart does not have a reasonable expectation of success as required by MPEP 2142 discussed above.

Based on the foregoing, Appellants respectfully submit that the rejection of each of Appellants' independent claims 1, 8, and 14 over Lewis in view of Lockhart has been overcome. Therefore, claims 1, 8, and 14 are allowable over Lewis in view of Lockhart. Claims 5, 11, 18, 21-26, and 28-30 each depend, directly or indirectly, on one of the allowable independent claims 1, 8, and 14. Therefore, each of these claims is allowable over Lewis in view of Lockhart for at least the same reasons that the independent claims are allowable.

2. **Claims 21, 23, and 25 Are Patentable over Lewis in view of Lockhart and further in view of Carlson.**

Claims 21, 23, and 25 each depend upon allowable independent claims 1, 8, and 14, respectively. The Examiner rejected these claims using Lewis in view of Lockhart and further in view of Carlson. The Examiner does not suggest, however, that Carlson teaches or suggests the limitations of claim 1, and indeed Carlson does not teach such limitations. Therefore, each of claims 21, 23, and 25 are allowable over Lewis in view of Lockhart and further in view of Carlson for at least the same reasons that their respective independent claims are allowable as discussed above.

3. **Claims 22, 24, and 26 Are Patentable over Lewis in view of Lockhart and further in view of Porras.**

Claims 22, 24, and 26 each depend upon allowable independent claims 1, 8, and 14, respectively. The Examiner rejected these claims using Lewis in view of Lockhart and further in view of Porras. The Examiner does not suggest, however, that Porras teaches or suggests the limitations of claim 1, and indeed Carlson does not teach such limitations. Therefore, each of claims 21, 23, and 25 are allowable over Lewis in view of Lockhart and further in view of Porras for at least the same reasons that their respective independent claims are allowable as discussed above.

4. **Claim 27 is Patentable over Ptacek in view of Lockhart and further in view of Barrett**

Independent claim 27 claims a method for preventing malicious network attacks on a server computer from a client computer that accesses the server computer via a computer network. Claim 27 includes the limitations of:

1) executing a test script that includes one or more attack simulations from the client computer, the execution of the test script including:

2) receiving, at the server computer, one or more packets from the client computer and one or more open socket requests form the client computer;

3) deciding a packet threshold for the client computer, the deciding including:

4) determining a number of packets received from the client computer during a time interval;

5) incrementing the number of packets received from the client computer; and

6) comparing the number of packets received with a packet limit stored at the server computer;

7) computing an open socket threshold for the client computer, the computing including:

8) determining a number of opened sockets for the client computer;

9) incrementing the number of opened sockets for the client computer;

10) comparing the number of sockets opened from the client computer to a socket limit stored at the server computer; and

11) evaluating the packet limit and the socket limit used during the attack simulations, the evaluating including:

12) analyzing the performance of the server computer during the simulation; and

13) **adjusting a server configuration setting** based on the analysis, wherein the adjusted server configuration setting is selected from group consisting of the stored packet limit and the stored socket limit.

The Examiner contends that Ptacek teaches the above limitations of claim 27. However, after further review of Ptacek, Ptacek does not teach or suggest such limitations. The excerpt from Ptacek that the Final Office Action uses to reject claim 27's limitations above states:

> "The system implements methodology providing a Custom Attack Simulation Language (CASL) that serves as an exploration tool for network protocols…. Since networks work by exchanging packets of information, CASL focuses on allowing users to read and write packets directly to and from the network. CASL functions as a scripting language-a high level programming language, like Perl, Python, or TEL… CASL is intended primarily for security auditing applications; that is to say, CASL is intended to simulate attacks against hosts in order to see if those hosts are vulnerable to attacks of a given nature…" (col. 6, lines 29-44).

As can be seen from the above excerpt, Ptacek teaches sending packets over a computer network for auditing purposes, but never teaches or suggests "adjusting a server configuration setting based on the analysis, wherein the adjusted server configuration setting is selected from group consisting of the stored packet limit and the stored socket limit" as claimed by Appellants. The Examiner does not suggest that Lockhart or Barret teach or suggest Appellants' "adjusting" step, and indeed they do not.

Based on the foregoing, Appellants respectfully submit that the rejection of Appellants' independent claim 27 over Ptacek in view of Lockhart and further in view of Barrett has been overcome. Therefore, since Ptacek, Lockhart, and Barret, either alone or in combination with each other, do not teach or suggest all the limitations included in claim 27, claim 27 is allowable over Ptacek in view of Lockhart and further in view of Barret.

Conclusion

For the foregoing reasons, Appellants respectfully submit that claims 1, 5, 8, 11, 14, 18, and 21-30 are patentable, and, accordingly, Appellants respectfully request that the Examiner's claim rejections be reversed and claims 1, 5, 8, 11, 14, 18, and 21-30 be allowed.

Respectfully submitted,

By /Leslie A. Van Leeuwen, Reg. No. 42,196/
Leslie A. Van Leeuwen, Reg. No. 42,196
Van Leeuwen & Van Leeuwen
Attorney for Appellants
Telephone: (512) 301-6738
Facsimile: (512) 301-6742

I. CLAIMS APPENDIX

1. A method for preventing malicious network attacks said method comprising:
providing a test script, the test script including one or more attack simulations;
processing the attack simulations included in the test script;
determining whether to change one or more configuration settings based upon the processing;
changing one or more of the configuration settings based upon the determination;
receiving a packet from a client computer;
identifying the client computer by a source IP address;
calculating a number of packets received using the source IP address during a time interval, wherein the calculating includes:
retrieving a number of packets received that correspond to the source IP address; and
incrementing the number of packets received;
comparing the incremented number of packets received with one or more of the configuration settings;
determining an action from a plurality of actions based on the comparing; and
executing the action.

2. (Canceled)

3. (Canceled)

4. (Canceled)

5. The method described in claim 1 further comprising:
receiving a socket request from the client computer;
determining a number of sockets opened for the client computer;
comparing the number of sockets opened to a socket limit; and
determining whether to allow a socket request based on the comparison.

6. (Canceled)

7. (Canceled)

8. An information handling system comprising:

one or more processors;

a memory accessible by the processors;

one or more nonvolatile storage devices accessible by the processors;

a network interface for receiving packets from a computer network; and

a packet handling tool to manage packets received from the network interface, the packet handling tool including:

means for providing a test script, the test script including one or more attack simulations;

means for processing the attack simulations included in the test script;

means for determining whether to change one or more configuration settings based upon the processing;

means for changing one or more of the configuration settings based upon the determination;

means for receiving a packet from a client computer through the network interface;

means for identifying the client computer by a source IP address;

means for calculating a number of packets received using the source IP address during a time interval, wherein the calculating includes:

means for retrieving a number of packets received that correspond to the source IP address; and

means for incrementing the number of packets received;

means for comparing the incremented number of packets received with one or more of the configuration settings;

means for determining an action from a plurality of actions based on the comparing; and

means for executing the action.

9. (Canceled)

10. (Canceled)

11. The information handling system as described in claim 8 further comprising:

means for receiving a socket request from the client computer;

means for determining a number of sockets opened for the client computer;

means for comparing the number of sockets opened to a socket limit; and

means for determining whether to allow a socket request based on the comparison.

12. (Canceled)

13. (Canceled)

14. A computer program product stored on a computer operable media, the computer operable media containing instructions for execution by a computer, which, when executed by the computer, cause the computer to implement a method for preventing malicious attacks, the method comprising:

providing a test script, the test script including one or more attack simulations;

processing the attack simulations included in the test script;

determining whether to change one or more configuration settings based upon the processing;

changing one or more of the configuration settings based upon the determination;

receiving a packet from a client computer through the network interface;

identifying the client computer by a source IP address;

calculating a number of packets received using the source IP address during a time interval, wherein the calculating includes:

retrieving a number of packets received that correspond to the source IP address; and

incrementing the number of packets received;

comparing the incremented number of packets received with one or more of the configuration settings;

determining an action from a plurality of actions based on the comparing; and

executing the action.

15. (Canceled)

16. (Canceled)

17. (Canceled)

18. The computer program product described in claim 14 wherein the method further comprises:
receiving a socket request from the client computer;
determining a number of sockets opened for the client computer;
comparing the number of sockets opened to a socket limit; and
means for determining whether to allow a socket request based on the comparison.

19. (Canceled)

20. (Canceled)

21. The method of claim 1 wherein the configuration settings include a first limit and a second limit, the method further comprising:
determining that the incremented number of packets exceeds the first limit;
processing the packet and sending a notification in response to determining that the incremented number of packets exceeds the first limit;
receiving a subsequent packet from the client computer;
incrementing again the number of packets in response to receiving the subsequent packet;
determining that the incremented again number of packets exceeds the second limit; and
rejecting the subsequent packet in response to determining that the incremented again number of packets exceeds the second limit.

22. The method of claim 1 wherein the configuration settings include a historical usage corresponding to the client computer, the method further comprising:
determining that the incremented number of packets is higher than the historical usage; and
sending a notification in response to determining that the incremented number of packets is higher than the historical usage.

23. The information handling system of claim 8 wherein the configuration settings include a first limit and a second limit, the information handling system further comprising:
means for determining that the incremented number of packets exceeds the first limit;
means for processing the packet and sending a notification in response to determining that the incremented number of packets exceeds the first limit;

means for receiving a subsequent packet over the network interface from the client computer;

means for incrementing again the number of packets in response to receiving the subsequent packet;

means for determining that the incremented again number of packets exceeds the second limit; and

means for rejecting the subsequent packet in response to determining that the incremented again number of packets exceeds the second limit.

24. The information handling system of claim 8 wherein the configuration settings include a historical usage corresponding to the client computer, the information handling system further comprising:

means for determining that the incremented number of packets is higher than the historical usage; and

means for sending a notification in response to determining that the incremented number of packets is higher than the historical usage.

25. The computer program product of claim 14 wherein the configuration settings include a first limit and a second limit, the method further comprising:

determining that the incremented number of packets exceeds the first limit;

processing the packet and sending a notification in response to determining that the incremented number of packets exceeds the first limit;

receiving a subsequent packet from the client computer;

incrementing again the number of packets in response to receiving the subsequent packet;

determining that the incremented again number of packets exceeds the second limit; and

rejecting the subsequent packet in response to determining that the incremented again number of packets exceeds the second limit.

26. The computer program product of claim 14 wherein the configuration settings include a historical usage corresponding to the client computer, the method further comprising:

determining that the incremented number of packets is higher than the historical usage; and

sending a notification in response to determining that the incremented number of packets is higher than the historical usage.

27. A method for preventing malicious network attacks on a server computer from a client computer that accesses the server computer via a computer network, said method comprising:

executing a test script that includes one or more attack simulations from the client computer, the execution of the test script including:

receiving, at the server computer, one or more packets from the client computer and one or more open socket requests form the client computer;

deciding a packet threshold for the client computer, the deciding including:

determining a number of packets received from the client computer during a time interval;

incrementing the number of packets received from the client computer; and

comparing the number of packets received with a packet limit stored at the server computer;

computing an open socket threshold for the client computer, the computing including:

determining a number of opened sockets for the client computer;

incrementing the number of opened sockets for the client computer;

comparing the number of sockets opened from the client computer to a socket limit stored at the server computer; and

evaluating the packet limit and the socket limit used during the attack simulations, the evaluating including:

analyzing the performance of the server computer during the simulation; and

adjusting a server configuration setting based on the analysis, wherein the adjusted server configuration setting is selected from group consisting of the stored packet limit and the stored socket limit.

28. The method of claim 1 wherein at least one of the configuration settings are selected from the group consisting of a number of packets allowed, a time interval, a server port, and an overcount action.

29. The information handling system of claim 8 wherein at least one of the configuration settings are selected from the group consisting of a number of packets allowed, a time interval, a server port, and an overcount action.

30. The computer program product of claim 14 wherein at least one of the configuration settings are selected from the group consisting of a number of packets allowed, a time interval, a server port, and an overcount action.

.

J. EVIDENCE APPENDIX

Not applicable.

K. RELATED PROCEEDINGS APPENDIX

Not applicable.